Дискретная математика

Тема: Множества

- Д.э.н. Л.В. Кальянов

Введение

Дискретная математика – направление в математике, объединяющее отдельные её разделы, ранее сформированные как самостоятельные теории. К ним относятся математическая логика и теории множеств, графов, кодирования, автоматов.

Дискретной математикой называют совокупность математических дисциплин, изучающих свойства математических моделей объектов, процессов, зависимостей, существующих в реальном мире, которыми оперируют в различных областях знаний.

Дискретная математика использует средства, разработанные в классической математике. Однако характер объектов, исследуемых дискретной математикой, настолько разнообразен, что методов классической математики не всегда достаточно для их изучения. Поэтому те специфические методы, которые применяют для очень широкого класса *конечных* дискретных (имеющих прерывный характер) объектов, и были объединены в общее направление – дискретную математику.

В настоящее время знание дискретной математики необходимо специалистам в различных областях деятельности.

- В данном курсе можно выделить три главные линии.
- Во-первых, в курсе изучаются так называемые основания математики (теория множеств и математическая логика).
- Во-вторых– теоретические основы современной информатики(теория алгоритмов и вычислимых функций, теория кодирования, алгебра логики).
- В третьих– те факты, методы и конструкции дискретной математики, которые применяются в экономико-математических моделях.

1.1. Общие понятия теории множеств

Совокупность элементов, объединённых некоторым признаком, свойством, составляет понятие **множество**. Например, *множество* книг в библиотеке, *множество* студентов в группе, *множество* натуральных чисел N и т.д.

Запись $a \in M$ означает: элемент *a* *принадлежит* множеству *M*, т. е. элемент *a* обладает некоторым признаком. Аналогично $a \notin M$ читается: элемент *a* *не принадлежит* множеству *M*.

Изображение множеств

Множества удобно изображать с помощью *кругов Эйлера*.

Множество *K* на рис. 1.1 называют **подмножеством** множества *M* и обозначают $K \subset M$.

Множество *K* называется **подмножеством** множества *M* ($K \subset M$), если для любого $x \in K$ выполняется $x \in M$.

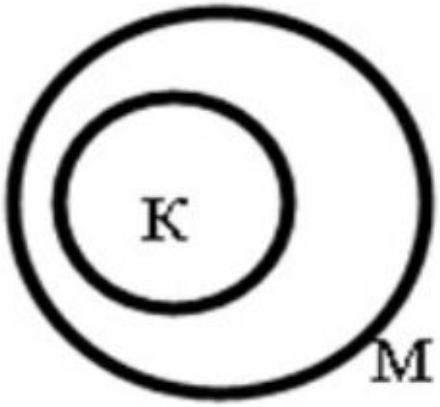


Рис. 1.1.

Универсальным называется множество *U*, состоящее из всех возможных элементов, обладающих данным признаком.

Если множество не содержит элементов, обладающих данным признаком, то оно называется **пустым** и обозначается $\varnothing$.

Равными называют два множества *A* и *B*, состоящие из одинаковых элементов: $A = B$.

Число элементов множества *A* называется **мощностью** множества и обозначается $|A|$ или $n(A)$.

Множество, элементами которого являются подмножества множества *M*, называется *семейством множества M* или *булеаном* этого множества и обозначается *B(M).*

Мощность булеана множества *M вычисляется по формуле*

$$|B(M)| = 2^n ,$$

где *n – это мощность множества M.*

Пример. $M = \{y, x, a\}, n = 3, |B(M)| = 2^3 = 8,$

$$B(M) = \{\varnothing, \{y\}, \{x\}, \{a\}, \{y, x\}, \{x, a\}, \{y, a\}, \{y, x, a\}\}.$$

- Часто для обозначения булеана множества M используется выражение 2^M.
- А для мощности булеана выражение
- $$|2^M| = 2^{|M|}$$

Множество считается **заданным**, если *перечислены* все его элементы, или *указано свойство* , которым обладают те и только те элементы, которые принадлежат данному множеству. Само свойство называется **характеристическим**.

В качестве характеристического свойства может выступать указанная для этого свойства *порождающая процедура*, которая описывает способ получения элементов нового множества из уже полученных элементов или из других объектов.

Примеры задания множества

Множество всех чисел, являющихся неотрицательными степенями числа 2 можно задать:

а) перечислением элементов: $M_{2^n} = \{1,2,4,8,16,32,\ldots\}$;

б) указанием характеристического свойства:

$$M_{2^n} = \{2^i \mid i \in Z, i \geq 0\};$$

в) с помощью порождающей процедуры по *индуктивным* правилам:

$$1 \in M_{2^n};$$

если $k \in M_{2^n}$, то $(2k) \in M_{2^n}$.

- В общем случае, множество A по схеме свертывания определяется как множество, которое содержит все элементы из K, обладающие свойством F.
- A = {x| x обладает свойством F}.

- Применяя сокращение F(x) для обозначения того, что элемент x обладает свойством F, будем писать
- $A = \{x \mid F(x)\}$.
- Очевидно, что $F(x) \in \{0,1\}$.
- **F(x) называется предикатом**.
- **Предика́т** (лат. *praedicatum* — заявленное, упомянутое, сказанное) — это то, что утверждается о субъекте.
  Субъектом высказывания называется то, о чём делается утверждение.

- Неограниченное применение схемы свертывания ведет к противоречиям. Например, можно получить «множество всех множеств»:
- M= {x| x– множество}.
- Если считать M множеством, то получаем M∈M.
- Рассмотрим парадокс Рассела, открытый в1902 году.

- Назовем множество правильным, если оно не является своим элементом, и неправильным в противном случае. Определим множество R как множество всех правильных множеств. Более формально:
- $R = \{x \mid x \notin R\}$.

- В соответствии с определением для любого множества A справедливо утверждение:
- $A \in R$ тогда и только тогда, когда $A \notin A$.
- В частности, если считать R множеством, то его само можно взять в качестве A, но тогда мы придем к противоречию:
- $R \in R$ тогда и только тогда, когда $R \notin R$.

- Более подробно. Если R правильное, то есть не является своим элементом, то оно должно находиться в R, то есть быть своим элементом.
- Если же R неправильное, то оно является своим элементом, то есть содержится в R, но R содержит только правильные множества.
- Таким образом, R не может быть ни правильным, ни неправильным.

1.2. Основные операции над множествами

Суммой или *объединением* двух множеств X и Y называется множество, состоящее из элементов, входящих или во множество X, или во множество Y, а может в оба множества одновременно (рис. 1.2). Обозначение: $Z=X\bigcup Y.$

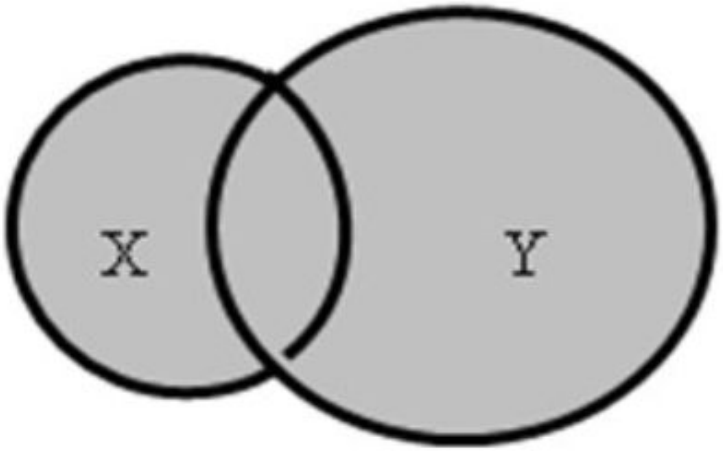


Рис. 1.2

Пересечением множеств X и Y называется множество, состоящее из элементов, входящих одновременно и во множество X, и во множество Y (рис. 1.3). Обозначение: $Z = X \bigcap Y.$

Разностью множеств X и Y называется множество Z, содержащее все элементы множества X, не содержащиеся в Y (рис. 1.4); эта разность обозначается $Z = X \setminus Y.$

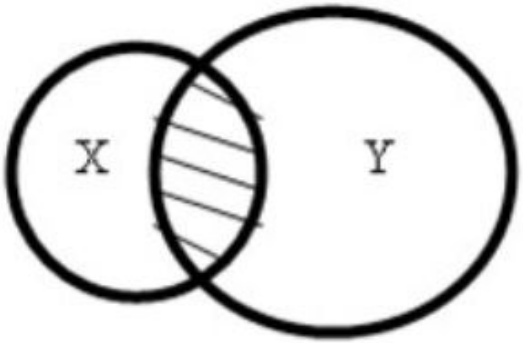


Рис. 1.3

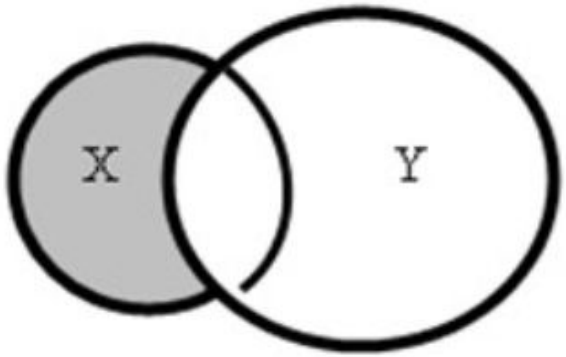


Рис. 1.4

Дополнением $\overline{X}$ множества X до универсального множества *U* *(рис. 1.5)* является множество

$$\overline{X} = \{x_i \mid x_i \notin X, x_i \in U\}.$$

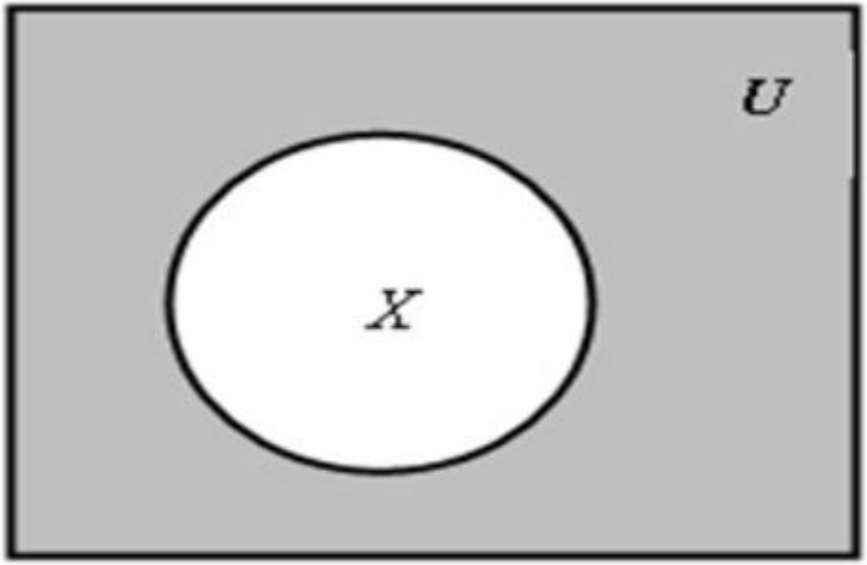


Рис. 1.5

Симметрической разностью множеств X и Y называется множество Z, содержащее либо элементы множества X, либо элементы множества Y, но не те и другие одновременно (*рис. 1.6*); эта разность обозначается $X \mathbin{\dot{\setminus}} Y$.

$$X \mathbin{\dot{\setminus}} Y = (X \setminus Y) \cup (Y \setminus X)$$

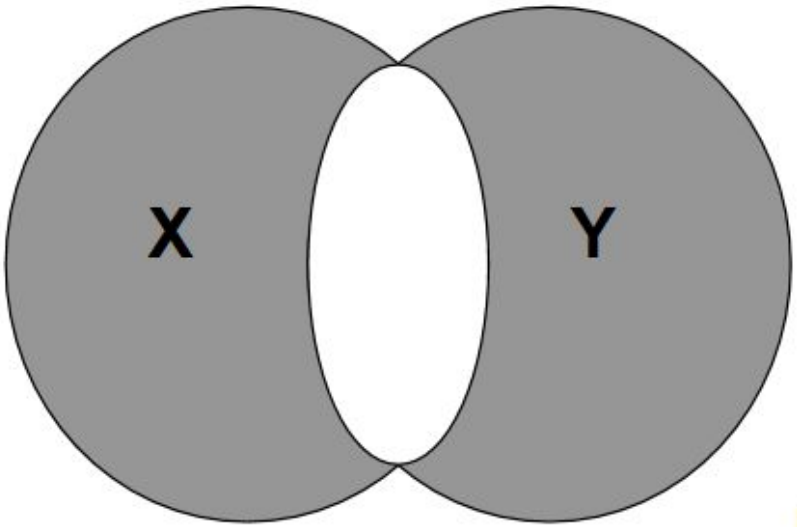


Рис. 1.6.

- Часто для обозначения симметрической разности используется обозначение
- $X \Delta Y$

Вместо выражения

«любое *x* из множества X»

можно писать $\forall x \in X$, где перевёрнутая латинская буква A взята от начала английского слова **Any** – любой.

Вместо выражения

«существует элемент *x* из множества X»

кратко пишут: $\exists x \in X$, где перевёрнутая латинская буква E является начальной в английском слове **Existence** – существование.

Множество A можно **разбить на классы** (непересекающиеся подмножества) A_i, если:

- объединение всех подмножеств совпадает с множеством A: $A = \bigcup_i A_i$;

- пересечение любых двух различных подмножеств пусто, т.е. для любых $i \neq j$ выполняется $A_i \bigcap A_j = \varnothing$.

Для операций над множествами справедливы следующие тождества:

- *законы коммутативности объединения и пересечения*

$$X \cup Y = Y \cup X, \quad X \cap Y = Y \cap X,$$

- *законы ассоциативности объединения и пересечения*

$$(X \cup Y) \cup Z = X \cup (Y \cup Z),$$
$$(X \cap Y) \cap Z = X \cap (Y \cap Z),$$

- *законы дистрибутивности пересечения относительно объединения и объединения относительно пересечения*

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z),$$
$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z);$$

- *законы поглощения*

$$X \cup (X \cap Y) = X, \quad X \cap (X \cup Y) = X;$$

- *законы склеивания*

$$(X \cap Y) \cup (X \cap \overline{Y}) = X, \quad (X \cup Y) \cap (X \cup \overline{Y}) = X;$$

- *законы Порецкого*

$$X \cup (\overline{X} \cap Y) = X \cup Y, \quad X \cap (\overline{X} \cup Y) = X \cap Y;$$

Операция $\cap$ имеет преимущество перед операцией $\cup$. Скобки - для наглядности.

- *законы идемпотентности объединения и пересечения* $X \cup X = X, \quad X \cap X = X;$
- *законы действия с универсальным (U) и пустым ($\varnothing$) множествами*

$$X \cup \varnothing = X, \qquad X \cap \varnothing = \varnothing,$$
$$X \cup U = U, \qquad X \cap U = X,$$
$$X \cup \overline{X} = U, \qquad X \cap \overline{X} = \varnothing;$$

- *законы де Моргана*

$$\overline{X \cap Y} = \overline{X} \cup \overline{Y}, \qquad \overline{X \cup Y} = \overline{X} \cap \overline{Y};$$

- *закон двойного дополнения*

$$\overline{\overline{X}} = X.$$

Пример. Проверим первый из законов де Моргана. Покажем сначала, что $\overline{A \cap B} \subset \overline{A} \cup \overline{B}$. Предположим, что $x \in \overline{A \cap B}$. Тогда $x \notin A \cap B$, так что x не принадлежит хотя бы одному из множеств A и B. Таким образом, $x \notin A$ или $x \notin B$, то есть $x \in \overline{A}$ или $x \in \overline{B}$. Это означает, что $x \in \overline{A} \cup \overline{B}$.

Мы показали, что произвольный элемент множества $\overline{A \cap B}$ является элементом множества $\overline{A} \cup \overline{B}$. Следовательно, $\overline{A \cap B} \subset \overline{A} \cup \overline{B}$. Обратное включение $\overline{A \cap B} \supset \overline{A} \cup \overline{B}$ доказывается аналогично. Достаточно повторить все шаги предыдущего рассуждения в обратном порядке.

1.3. Соответствия между множествами. Отображения

Пары (a_i, b_j) задают **соответствие** между множествами *A* и *B*, если указано правило *R*, по которому для элемента множества *A* выбирается элемент из множества *B*.

Пусть для некоторого элемента *a* множества *A* поставлен в соответствие некоторый элемент *b* из множества *B*, который называется **образом** элемента *a* и записывается $b = R(a)$. Тогда $a = R^{-1}(b)$ - **прообраз** элемента $b \in B$.

Образ множества *A* при соответствии *R* называется **множеством значений** этого соответствия и обозначается $R(A)$, если $R(A)$ состоит из образов всех элементов множества A:

$$R(A) = \{b \mid \forall a \in A, \exists b \in B : b = R(a)\}.$$

Прообраз множества *B* при некотором соответствии *R* называют **областью определения** этого соответствия и обозначают $R^{-1}(B)$ т.е.

$$R^{-1}(B) = \{a \mid \forall b \in B, \exists a \in A : R(a) = b\}.$$

R^{-1} является **обратным** соответствием для *R*.

Для описания соответствий между множествами используют понятие **отображения.**

Для задания отображения *f* необходимо указать:

- множество, которое отображается (**область определения** отображения, обозначается $D(f)$);
- множество, в (на) которое отображается область определения (**множество значений** этого отображения, обозначается $E(f)$);
- **закон** или соответствие между этими множествами, по которому для элементов первого множества выбраны элементы из второго.

При записи $f : A \to B$ подразумевается, что отображение *f* определено *всюду* на *A*, т.е. *A* – полный прообраз отображения *f*, хотя для *B* такое свойство полноты не подразумевается.

Однозначным называется отображение, где каждому аргументу поставлено в соответствие не более одного образа.

Отображения можно задавать:

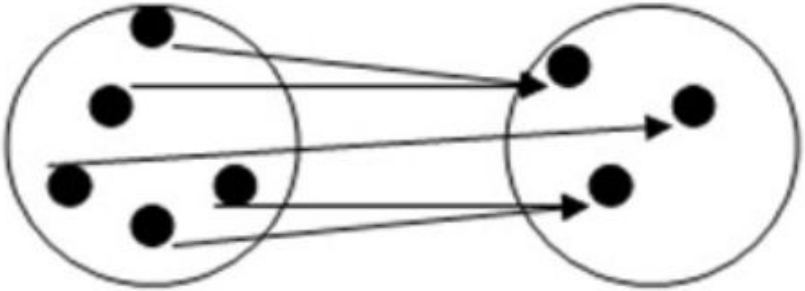
а) аналитически (с помощью формул);

б) графически (с помощью стрелочных схем);

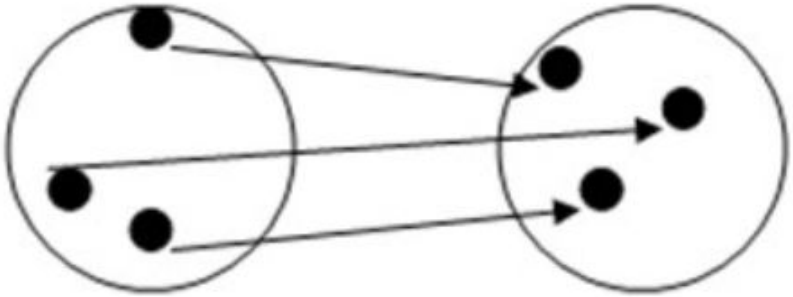
в) с помощью таблиц.

Классификация отображений по мощности

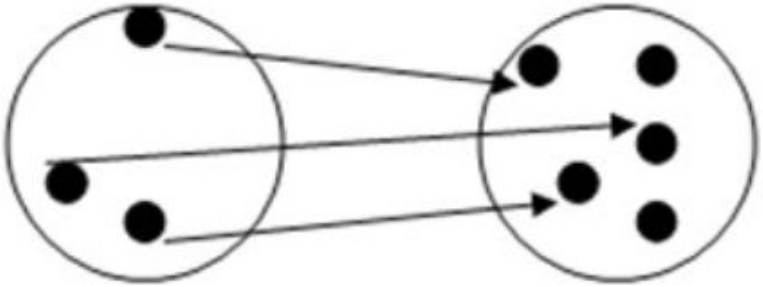
- На множество «сюръекция»;



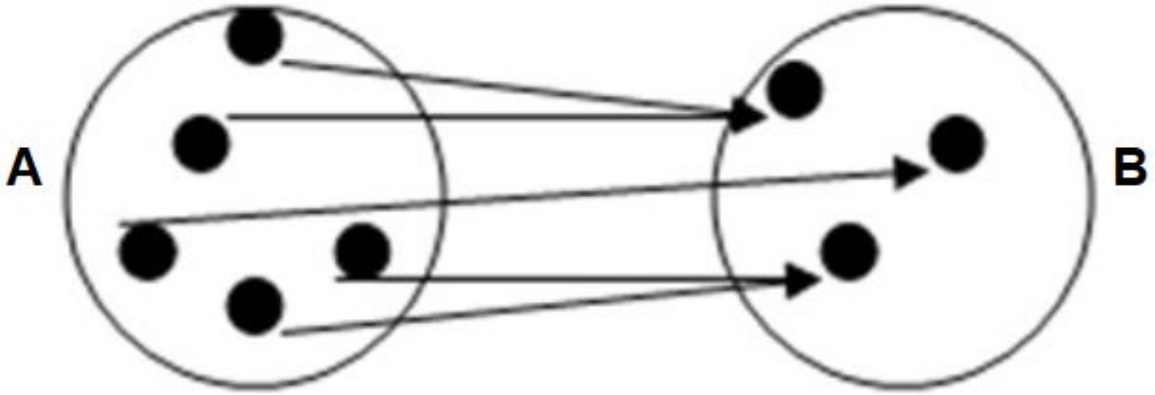
- На множество «биекция»;



- Во множество «инъекция».

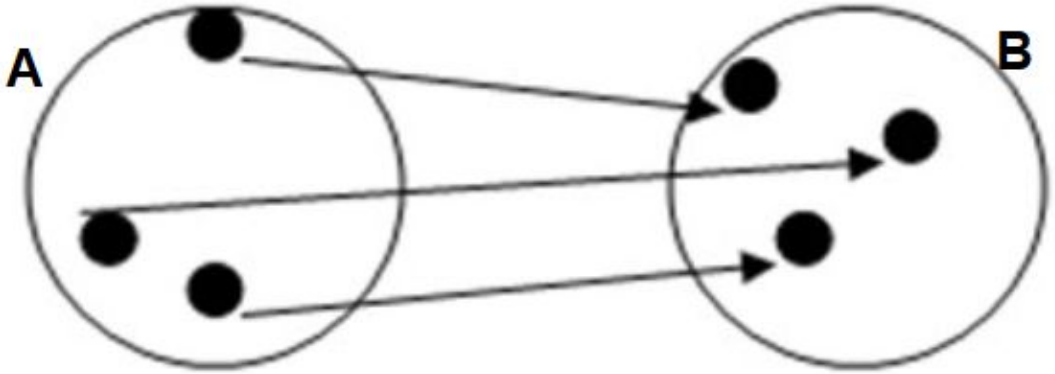


На множество - «сюръекция»



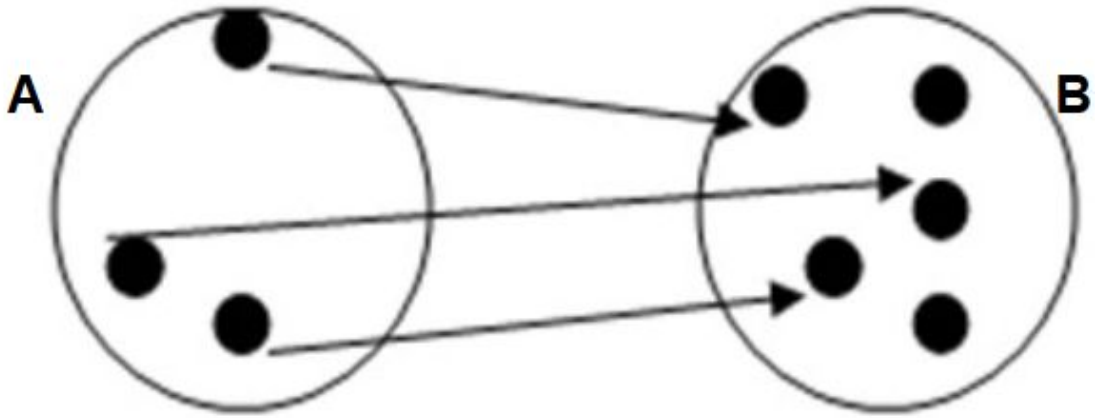
Соответствие. при котором каждому элементу множества *A* указан *единственный* элемент множества *B*, а каждому элементу множества *B* можно указать *хотя бы* один элемент множества *A*, называется отображением множества *A* **на** множество *B*

На множество - «биекция»



Отображение множества A **на** множество B, при котором каждому элементу множества B соответствует единственный элемент множества A, называется **взаимно-однозначным** соответствием между двумя множествами, или **биекцией**.

Во множество - «инъекция»



Соответствие. при котором каждому элементу множества *A* указан *единственный* элемент множества *B*, а каждому элементу *B* соответствует *не более* одного прообраза из *A*, называется отображением множества *A* **во** множество *B*.

Пусть множество *A* отображается *взаимно-однозначно* на множество *B*, т.е. $f:A\to B$. Тогда отображение , при котором каждому элементу множества *B* ставится в соответствие его прообраз из множества *A*, называется **обратным отображением** для *f* и записывается $B\xrightarrow{f^{-1}}A$ или $f^{-1}:B\to A$.

Если между элементами множеств установлено взаимнооднозначное соответствие, то эти множества **равносильны**, **равномощны**, или **эквивалентны**.

1.4. Классификация множеств. Мощность множества

Множество, содержащее конечное число элементов, называется **конечным**. Пустое множество является *конечным* и имеет мощность, равную нулю, т.е. $|\varnothing| = 0.$ Множество, не являющееся конечным, называется **бесконечным**.

Бесконечное множество, эквивалентное множеству натуральных чисел N, называется **счётным**. В противном случае бесконечное множество будет **несчётным**.

Основная теорема о конечных множествах

Теорема. Любое конечное множество не эквивалентно никакому его собственному подмножеству, кроме самого себя.

Следствие. Всякое непустое конечное множество эквивалентно одному и только одному отрезку натурального ряда чисел $[1, n]$.

Счётными являются множество Z целых чисел и Q рациональных чисел. Множество R действительных чисел *несчётно* .

Множество действительных чисел называется множеством *мощности континуума* (от лат. continuum – непрерывный).

1.5. Кортежи. Декартовы произведения

Кортежем длины *n* из элементов множества *A* называется упорядоченная последовательность $\langle a_1, a_2, \ldots, a_n \rangle$ элементов этого множества.

Кортежи $\langle a_1, a_2, \ldots, a_k \rangle$ и $\langle b_1, b_2, \ldots, b_n \rangle$ называются **равными**, если они имеют одинаковую длину и их элементы с одинаковыми номерами совпадают, т. е. $\langle a_1, a_2, \ldots, a_k \rangle = \langle b_1, b_2, \ldots, b_n \rangle$, если $(k = n)$ и для $\forall i \quad a_i = b_i$.

В отличие от элементов множества элементы кортежа могут совпадать.

Например, в прямоугольной системе координат координаты точек являются кортежами.

Операция, с помощью которой из двух кортежей длиной k и m можно составить новый кортеж длиной $k + m$, в котором сначала идут подряд элементы первого кортежа, а затем – элементы второго кортежа, называется **соединением кортежей**.

Существуют кортежи, элементы которых являются только нулями или единицами.

Кортеж из нулей и единиц можно рассматривать как *двоичное представление натурального числа*.

Кортеж, состоящий из единиц и нулей, описывает *состояние памяти вычислительных машин*, причём память может содержать числа, тексты, команды и т.д.

Кортежи используются в штрих-кодах для сообщения нужной информации о характеристике объекта (белая полоска определённой ширины – 0, чёрная -1).

Декартово произведение

Декартовым (прямым) произведением множеств $A_1, A_2, \ldots, A_n$ называется множество $A_1 \times A_2 \times \ldots \times A_n$, состоящее из всех кортежей $\langle a_1, a_2, \ldots, a_n \rangle$ длины *n*, в которых $a_k \in A_k$, где $1 \le k \le n$.

$$|A_1 \times \ldots \times A_n| = |A_1| \times \ldots \times |A_n|$$

Пример. $A_1 = \{1,2\}$, $A_2 = \{3,4\}$, $A_1 \times A_2 = \{\langle 1,3\rangle, \langle 1,4\rangle, \langle 2,3\rangle, \langle 2,4\rangle\}$

Если $A_1 = A_2 = \ldots = A_n = A$, то пишут $A^n = \underbrace{A \times A \times \ldots \times A}_{n}$

A^n называют ***n*-й декартовой степенью** множества *A*. $|A^n| = |A|^n$

Отношения. Бинарные отношения и их свойства

Подмножество $R \subset M^n$ называется ***n*-местным отношением** *R* на непустом множестве *M*. При *n*=2 отношение *R* называется **бинарным**.

- Для обозначения бинарного отношения R на множестве M, будем использовать как обозначение
  - $(a,b) \in R$,
- так и обозначение
  - aRb,
- где $a \in M$, $b \in M$

Свойства бинарных отношений:

рефлексивность:

$$(\forall a \in M)((a,a) \in R)$$

антирефлексивность:

$$(\forall a \in M)((a,a) \notin R)$$

Отношения. Бинарные отношения и их свойства

Подмножество $R \subset M^n$ называется ***n*-местным отношением** *R* на непустом множестве *M*. При *n*=2 отношение *R* называется **бинарным**.

Свойства бинарных отношений:

рефлексивность:

$$(\forall a \in M)((a,a) \in R)$$

антирефлексивность:

$$(\forall a \in M)((a,a) \notin R)$$

транзитивность:

$$(\forall a,b,c \in M)(((a,b) \in R, (b,c) \in R) \rightarrow (a,c) \in R)$$

антитранзитивность:

$$(\forall a,b,c \in M)(((a,b) \in R, (b,c) \in R) \rightarrow (a,c) \notin R)$$

связность:

$$(\forall a,b \in M)((a,b) \in R \text{ или } (b,a) \in R)$$

Каждое конкретное отношение может обладать или не обладать указанным свойством.

Примеры рефлексивных отношений:

«быть не больше»; «быть делителем» на множестве N; «быть коллинеарным» на множестве векторов;

Примеры антирефлексивных отношений:

«быть больше»; «быть младше»; «быть перпендикулярной» на множестве прямых;

Примеры симметричных отношений:

«быть перпендикулярным»; «быть равным»; «быть параллельным»;

Примеры антисимметричных отношений:

«быть меньше или равным»; «быть делителем»; «быть подмножеством»;

Примеры асимметричных отношений;

«быть больше»; «быть меньше»; «быть отцом»;

Примеры транзитивных отношений:

«быть больше»; «быть меньше»; «быть равным»;

Примеры антитранзитивных отношений:

«быть перпендикулярным» на множестве прямых плоскости; «быть сыном»; «жить этажом выше» для жильцов дома.

Примеры отношений связности:

«быть больше», «быть меньше» на множестве N, R; «быть больше или равным», «быть меньше или равным» на множестве обыкновенных дробей.

Примеры отношений эквивалентности:

Отношение «быть равным», «иметь один и тот же остаток от деления на конкретное число»

Непересекающиеся подмножества, на которые разбивается множество *M* отношением эквивалентности, называются классами эквивалентности.

На множестве обыкновенных дробей все классы эквивалентности по отношению равенства состоят из дробей, равных по своей величине.

На множестве треугольников все классы эквивалентности по отношению подобия состоят из треугольников, подобных между собой.

Пусть ρ — отношение эквивалентности на множестве A и $x \in A$. Множество всех элементов A, эквивалентных x, т.е. множество $\{y:\ y \rho x\}$, называют классом эквивалентности по отношению ρ и обозначают $[x]_\rho$. Отметим, что в силу рефлексивности для любого элемента $x \in A$ класс эквивалентности не пуст, так как $x \in [x]_\rho$.

Теорема 1.1. *Для любого от ношения эквивалент ност и на множест ве A множест во классов эквивалент ност и образует разбиение множест ва A. Обрат но, любое разбиение множест ва A задает на нем от ношение эквивалент ност и, для кот орого классы эквивалент ност и совпадают с элемент ами разбиения.*

Покажем, что **отношение эквивалентности** ρ на множестве A определяет некоторое разбиение этого множества. Убедимся вначале, что любые два класса эквивалентности по отношению ρ либо не пересекаются, либо совпадают.

Пусть два класса эквивалентности $[x]_\rho$ и $[y]_\rho$ имеют общий элемент $z \in [x]_\rho \cap [y]_\rho$. Тогда $z \rho x$ и $z \rho y$. В силу симметричности отношения ρ имеем $x \rho z$, и тогда $x \rho z$ и $z \rho y$. В силу транзитивности отношения ρ получим $x \rho y$. Пусть $h \in [x]_\rho$, тогда $h \rho x$. Так как $x \rho y$, то $h \rho y$ и, следовательно, $h \in [y]_\rho$.

Обратно, если $h \in [y]_\rho$, то в силу симметричности ρ получим $h \rho y,\ y \rho x$ и в силу транзитивности — $h \rho x$, то есть $h \in [x]_\rho$. Таким образом, $[x]_\rho = [y]_\rho$.

Итак, любые два не совпадающих класса эквивалентности не пересекаются. Так как для любого $x \in A$ справедливо $x \in [x]_\rho$ (поскольку $x \rho x$), т.е. каждый элемент множества A принадлежит некоторому классу эквивалентности по отношению ρ, то множество всех классов эквивалентности по отношению ρ образует разбиение исходного множества A. Таким образом, любое отношение эквивалентности однозначно определяет некоторое разбиение.

Теперь пусть $(B_i)_{i \in I}$ — некоторое разбиение множества A. Рассмотрим отношение ρ, такое, что $x \rho y$ имеет место тогда и только тогда, когда x и y принадлежат одному и тому же элементу B_i данного разбиения:

$$x \rho y \Leftrightarrow (\exists i \in I)(x \in B_i) \wedge (y \in B_i).$$

Очевидно, что введенное отношение рефлексивно и симметрично. Если для любых x, y и z имеет место $x \rho y$ и $y \rho z$, то x, y и z в силу определения отношения ρ принадлежат одному и тому же элементу B_i разбиения. Следовательно, $x \rho z$ и отношение ρ транзитивно. Таким образом, ρ — эквивалентность на A.

Теорема 1.1 позволяет отождествлять отношения эквивалентности и разбиения: любая эквивалентность определяет единственное разбиение и наоборот.

Множество всех классов эквивалентности по данному отношению эквивалентности ρ на множестве A называют фактор-множеством множества A по отношению ρ и обозначают A/ρ.

Пример . На множестве целых чисел $\mathbb{Z}$ определим отношение равенства по модулю k, где $k \in \mathbb{N}$. Положим $x =_{(\mathrm{mod}\, k)} y$, если и только если $(x - y)$ делится на k.

Легко проверяется, что это отношение эквивалентности. Действительно, рефлексивность следует из того, что для любо $m \in \mathbb{Z} m - m = 0$ и делится на k; симметричность — из того, что если $(m - n)$ делится на k, то и $(n - m)$ делится на k.

Для доказательства транзитивности заметим, что если $(m-n)$ делится на k и $(n-p)$ делится на k, то и их сумма $(m-n)+(n-p)=m-p$ делится на k. Другими словами, для любых целых m, n, p из $m =_{(\mathrm{mod}\, k)} n$ и $n =_{(\mathrm{mod}\, k)} p$ следует $m =_{(\mathrm{mod}\, k)} p$, что доказывает транзитивность отношения $=_{(\mathrm{mod}\, k)}$.

Равенство чисел m и n по модулю k означает, что при делении на k эти числа дают одинаковые остатки.
Действительно, для каждого $x \in \mathbb{Z}$ имеем $x = m \cdot k + r$, где $r -$ остаток от деления xна k.

Следовательно, $x - r = m \cdot k$, то есть $x =_{(\mathrm{mod}\, k)} r$. Таким образом, каждое число попадает в тот же класс эквивалентности по отношению $=_{(\mathrm{mod}\, k)}$, что и остаток от деления его на k. Поскольку всего различных остатков может быть ровно k: $0, 1, \ldots, k-1$, получаем ровно k попарно различных классов эквивалентности по данному отношению:

$$[0] =_{(\mathrm{mod}\, k)}, \quad [1] =_{(\mathrm{mod}\, k)}, \quad \ldots, \quad [k-1] =_{(\mathrm{mod}\, k)},$$

где класс $[r]_{=(\mathrm{mod}\,k)}$ состоит из всех целых чисел, дающих при делении на k остаток r.

Отметим, что мы установили взаимно однозначное соответствие между фактор-множеством $\mathbb{Z}/_{=(\mathrm{mod}\,k)}$ и множеством $\mathbb{Z}_k$, состоящим из чисел $0, 1, \ldots, k-1$.

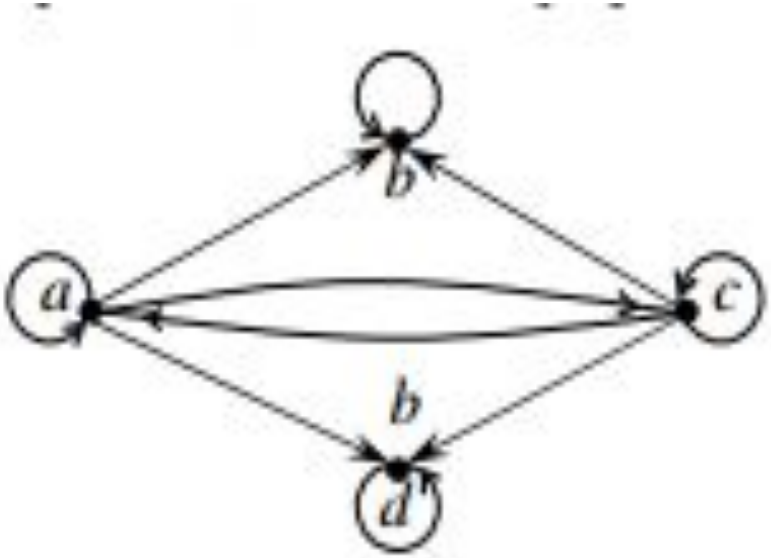
Второе множество дает нам как бы «наглядный образ» построенного фактор-множества. Нельзя считать, что фактор-множество $\mathbb{Z}/_{=(\mathrm{mod}\,k)}$ равно множеству $\{0, 1, \ldots, k-1\}$. Нет, указанное фактор-множество состоит из k элементов, каждый из которых есть не число, а множество всех целых чисел, при делении на k дающих фиксированный остаток.

Но каждому такому классу эквивалентности однозначно сопоставляется целое число от 0 до $k-1$, и, наоборот, каждому целому числу от 0 до $k-1$ соответствует единственный класс эквивалентности по отношению $=(\mathrm{mod}\, k)$.

Отношение порядка.

- Пусть A– непустое множество.
- Определение. Отношение $P \subseteq A$ называется предпорядком (квази-порядком), если оно рефлексивно и транзитивно.

Пример. Пусть A= {a, b, c, d}.
Отношение P= {(a, a), (a, b), (a, c), (a, d), (b, b), (c, a), (c, b), (c, c), (c, d), (d, d)} на множестве A является предпорядком.



- Определение. Отношение $P \subseteq A$ называется частичным порядком, если оно рефлексивно, транзитивно и антисимметрично. Таким образом, частичный порядок представляет собой антисимметричный предпорядок. Частичный порядок обозначается символом $\leq$.

- Определение. Отношение $< \subseteq A$ называется строгим порядком, если оно определяется по следующему правилу: $(\forall\ x, y \in A)\ x < y \Leftrightarrow x \leq y$ и $x \neq y$.
- Отношение строгого порядка не является частичным порядком, так как оно не рефлексивно.

- Определение. Пусть $\leq \subseteq A$ и $x, y \in A$. Элементы x и y называются несравнимыми, если нельзя сказать, что $x \leq y$ или $y \leq x$.
- Пример. Пусть $A = \{a, b, c, d\}$. Отношение включения $\subseteq$ на булеане $P(A)$ является частичным порядком. Элементы $B = \{a, c\}$ и $C = \{b, d\}$ из $P(A)$
- являются несравнимыми, так как$(B, C) \notin \subseteq$ и $(C, B) \notin \subseteq$.

- Определение. Частичный порядок $\leq \subseteq A$ называется линейным порядком, если$(\forall\ x, y \in A)\ x \leq y$ или $y \leq x$.
- Определение. Пусть $A \neq \varnothing$ и $\leq$– частичный(линейный) порядок на A.
- Упорядоченная пара $\langle A, \leq \rangle$ называется частично(линейно) упорядоченным множеством.

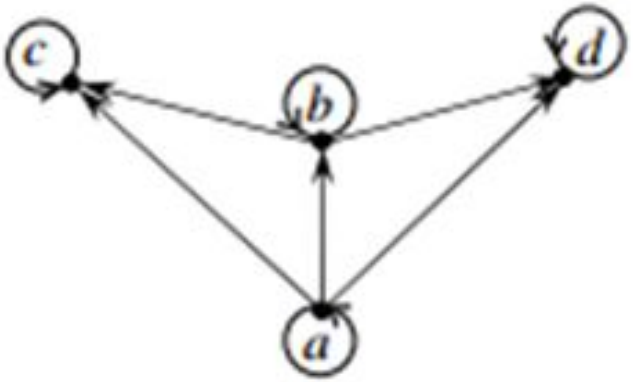
- Пример. Пара $< Z, \leq >$, где $\leq$– отношение делимости на множестве Z, является частичным, но не линейным порядком.
- Пары $< N, \leq >$, $< R, \leq >$ с обычными отношениями $\leq$ образуют линейно упорядоченные множества.

- Определение. Элемент $a \in A$ частично упорядоченного множества $< A, \leq >$ называется максимальным (минимальным), если $(\forall x \in A)\ a \leq x (x \leq a) \Rightarrow x = a$.
- Определение. Элемент $a \in A$ частично упорядоченного множества $< A, \leq >$ называется наибольшим(наименьшим), если $(\forall\ x \in A)\ x \leq a (a \leq x)$.

- Наибольший(наименьший) элемент частично упорядоченного множества
- $< A, \leq >$(если он существует) обозначается через $\max A$ ($\min A$).

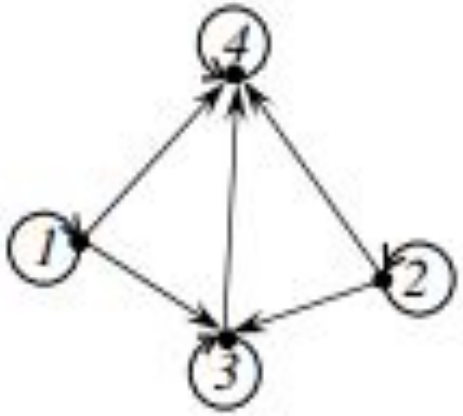
- Теорема. Пусть $< A, \leq >$ является частично упорядоченным множеством, где A– непустое и конечное множество. Тогда $< A, \leq >$ содержит хотя бы один минимальный элемент, и если он является единственным, то он также является и наименьшим. Аналогично, $< A, \leq >$ содержит хотя бы один максимальный элемент, и если он является единственным, то он также является наибольшим.

- Пример. Частично упорядоченное множество $< A, \leq >$, где
- $A = \{a, b, c, d\}$, а граф отношения $\leq$ изображен на рис.,



- имеет единственный минимальный и он же наименьший элемент a, максимальные элементы c и d, но не имеет наибольшего элемента.

- Пример3.22. Частично упорядоченное множество < B, ≤ >, где
- B= {1, 2, 3, 4}, а граф отношения ≤ изображен на рис. 3.8,



- имеет минимальные элементы 1 и 2, единственный максимальный и он же наибольший элемент4, но не имеет наименьшего элемента.

- Замечание. Всякий наибольший элемент частично упорядоченного множества является максимальным, а всякий наименьший элемент – минимальным. Обратное утверждение, вообще говоря, неверно.

Отношение эквивалентности – частный случай отношения толерантности.

Отношения «быть другом», «быть знакомым», - отношения толерантности, так как они рефлексивны, симметричны, но не транзитивны.

Отношение «иметь непустое пересечение» для множеств – отношение толерантности.


Отношение порядка
антисимметричность
транзитивность
Множество М, которое обладает отношением порядка, называется упорядоченным.
+ рефлексивность
Отношение нестрогого порядка ≤
+ антирефлексивность
Отношение строгого порядка <

Отношение называется отношением полного порядка, если сравнимы все элементы множества, на котором задано это отношение.

Пример. Отношения «больше» и «меньше» на множестве действительных чисел.

Отношение называется отношением частичного порядка, если сравнимы не все элементы множества, на котором задано это отношение.

Пример. Отношение «быть подмножеством» на множестве B(U) (булеан).

Операции над отношениями

- Так как отношения, заданные на фиксированной паре множеств являются подмножества множества A×B, то можно определить операции объединения, пересечения и дополнения отношений.

Для произвольных $a \in A, b \in B$:

$$a\,(R \cup S)\,b \Leftrightarrow a\,R\,b \vee a\,S\,b,$$
$$a\,(R \cap S)\,b \Leftrightarrow a\,R\,b \wedge a\,S\,b,$$
$$a\,\overline{R}\,b \Leftrightarrow \neg a\,R\,b.$$

- Часто вместо объединения, пересечения и дополнения отношений говорят об их дизъюнкции, конъюнкции и отрицании.

Кроме перечисленных важное значение имеют ещё операции обращения и умножения отношений, определяемые следующим образом.

Если $R \subseteq A \times B$, то обратным отношением называется отношение R^{-1}, определённое на паре B, A и состоящее из тех пар (b, a), для которых $a\, R\, b$. Например, $(<)^{-1} = (\geqslant)$.

Пусть $R \subseteq A \times B, S \subseteq B \times C$. Композицией (или произведением) отношений R и S называется отношение $RS \subseteq A \times C$ такое, что:

$$a\, RS\, c \Leftrightarrow \exists b \in B\, a\, R\, b \wedge b\, S\, c.$$

Например, для отношения строгого порядка на множестве натуральных числе его умножение на себя определено следующим образом: $a(<)(<)b \Leftrightarrow a+1<b$.

Бинарные отношения R и S называются перестановочными, если $RS = SR$.

Отношение $\rho \subseteq A \times B$ называют функциональным по второй (первой) компоненте,
если для любых двух упорядоченных пар
$(x, y) \in \rho$ и $(x' y') \in \rho$
из равенства $x = x'$ следует $y = y'$
(и из $y = y'$ следует $x = x'$).

Функциональность соответствия по второй компоненте означает, что, фиксируя в любой упорядоченной паре, принадлежащей данному соответствию, первую компоненту, мы однозначно определяем и вторую компоненту.
Таким образом, мы можем сказать, что соответствие, функциональное по второй компоненте, есть отображение (возможно, частичное).

Поэтому соответствие $f \subseteq A \times B$ является отображением из A в B, если и только если оно всюду определено (т.е. $D(f) = A$) и функционально по второй компоненте.
Отметим также, что отображение из A в B является инъекцией тогда и только тогда, когда оно функционально по первой компоненте.

1.7. Элементы комбинаторики

Раздел математики, занимающийся подсчётами количества различных комбинаций между объектами, называется комбинаторикой.

Все комбинаторные задачи сводятся к подсчёту мощности конечных множеств и их отображений.

Правило суммы. Пусть элемент α можно выбрать k способами, а элемент β - m способами, причём, если любой способ выбора α отличается от любого способа выбора β, то выбор «α или β» можно сделать $k+m$ способами.

Пример. Если в группе 16 юношей и 14 девушек, то преподаватель может вызвать к доске одного учащегося 16 + 14 = 30 способами.

Правило произведения. Если элемент α можно выбрать *k* способами, а элемент β - *m* способами, то пару (α, β) можно выбрать $k \cdot m$ способами.

Пример. Для вызова к доске пары «юноша и девушка» существует16 · 14 = 224 способа.

Частный случай правила произведения – число размещений с повторениями $\overline{A}_m^k = m^k$ для подсчёта кортежей длины *k*, составленных из элементов множества X мощности *m*.

Перестановки. Упорядоченные множества (кортежи), состоящие из *n* различных элементов, называются перестановками (без повторений). Обозначение : P_n .

Формула для нахождения числа перестановок: $P_n = n! = nP_{n-1}$.

Задачи:

- Сколькими способами можно переставлять элементы множества, чтобы получить различные кортежи длины *n* ?
- Сколькими способами можно расфасовать *n* шаров разного цвета в ящик с *n* свободными местами ?

Пример. Из цифр 3, 5, 7, 9 можно составить 4! кортежей, так как $n=4$, то $P_4=4!=4\cdot3\cdot2\cdot1=24$, т.е. существует 24 различных четырёхзначных числа, составленных из этих цифр: 5379, 7359, 9375, … .

Формула $P_n = n! = nP_{n-1}$ называется *рекуррентной* и даёт возможность подсчитывать число перестановок во множестве $n+1$ элемента через перестановки во множестве n элементов.

$P_1=1!$, $P_0=0!=1$. Если во множестве один элемент, то кортеж единственный; если нет элементов, то вариант один – «нет кортежа».

Размещения (без повторений). Упорядоченное подмножество m элементов (кортеж), составленное из всего множества, содержащего n элементов, называется размещением (без повторения). Обозначение: A_n^m.

Формула для нахождения числа размещений:

$$A_n^m = \frac{n!}{(n-m)!}$$

Задачи.

- Сколькими способами из всего множества можно выбрать различные кортежи (упорядоченные подмножества) длиной m ($m < n$)?

Сочетания без повторений.

Сочетаниями из n элементов по m называется неупорядоченное подмножество (выборка), состоящее из m элементов, взятых из множества, состоящего из n элементов.

Обозначение: C_n^m .

Формула для подсчёта числа сочетаний:

$$C_n^m = \frac{n!}{m!(n-m)!}$$

Задачи.

• Сколькими способами из всего множества можно выбрать различные подмножества длиной m ($m < n$)?

Перестановки с повторениями . Кортеж, имеющий повторяющиеся элементы, называется перестановкой с повторениями.

Пусть в кортеже длины n первый элемент встречается n_1 раз, второй элемент – n_2 раз и так далее, элемент под номером m – n_m раз: $n_1+n_2+\ldots+n_m = n$. Тогда число перестановок с повторениями из этих n элементов обозначается $\overline{P}_{n_1,n_2,\ldots,n_m}$ и вычисляется по формуле:

$$\overline{P}_{n_1,n_2,\ldots,n_m} = \frac{n!}{n_1!n_2!..n_m!}$$

1.8. Подстановки

Дано множество $E_n = \{1,2,\ldots,n\}, \forall n \in N$.

Взаимнооднозначное отображение $\sigma: E_n \to E_n$ множества E_n на себя называется **подстановкой степени** *n*.

Если прообразы (аргументы) расположены в порядке возрастания, запись подстановки такого вида называется канонической.

Например,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 2 & 5 & 3 & 1 & 7 & 4 \end{pmatrix}.$$

Чтобы из подстановки получить обратную, нужно поменять местами образы и прообразы, т.е. верхнюю и нижнюю строчки, и, если требуется, привести к каноническому виду.

Например, если $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 2 & 5 & 3 & 1 & 7 & 4 \end{pmatrix}$, то

$$\sigma^{-1} = \begin{pmatrix} 6 & 2 & 5 & 3 & 1 & 7 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 4 & 7 & 3 & 1 & 6 \end{pmatrix}$$

Обратная подстановка единственная.

Если подстановка записана в каноническом виде, то первую строчку можно не писать.

Подстановку вида $\sigma = (1,2,\ldots n) = e$ называют тождественной, так как она каждый элемент множества отображает в этот же элемент.

Произведением подстановок σ_1 и σ_2 называется подстановка $\sigma = \sigma_2 \circ \sigma_1$, где сначала выполняется подстановка σ_1, а затем подстановка σ_2 действует на результат первой.

Натуральной степенью подстановки σ называется подстановка $\sigma^n = \underbrace{\sigma \cdot \ldots \cdot \sigma}_{n}$, т.е. произведение *n* подстановок σ.

Порядком подстановки называется наименьшее натуральное число λ, такое что $\sigma^{\lambda} = e$.

Например, для подстановки $\sigma=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 3 & 1\end{pmatrix}$ λ=3.

В подстановке любая перемена двух элементов второй строки местами называется транспозицией.

Подстановка называется чётной, если число транспозиций, приводящих эту подстановку к тождественной, чётно. В противном случае подстановка называется нечётной.

Пример.

Приведём подстановку σ к тождественной подстановке с помощью транспозиций.

$$\sigma=\begin{pmatrix}1&2&3&4&5&6\\6&4&3&1&2&5\end{pmatrix}\xrightarrow{1}\begin{pmatrix}1&2&3&4&5&6\\1&4&3&6&2&5\end{pmatrix}\xrightarrow{2}\begin{pmatrix}1&2&3&4&5&6\\1&2&3&6&4&5\end{pmatrix}\xrightarrow{3}$$

$$\xrightarrow{3}\begin{pmatrix}1&2&3&4&5&6\\1&2&3&4&6&5\end{pmatrix}\xrightarrow{4}\begin{pmatrix}1&2&3&4&5&6\\1&2&3&4&5&6\end{pmatrix}.$$

Чётное число транспозиций ($n = 4$) указывает на чётность подстановки.